UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The person of Kyle Scott Broadhurst, the Subject Vehicle, and the Subject Premises more fully described in Attachment A	)	Case No. 3:23-mc-394

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The person of Kyle Scott Broadhurst, any devices found on his person, including his cell phone, the Subject Vehicle, and the Subject Premises located at 11304 SE 60th Ave., Milwaukie, OR 97222, more fully described in Attachment A.

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of or Accessing with Intent to View Child Pornography

The application is based on these facts:

See the attached affidavit of HSI Special Agent Rachel Kessler.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rachel Kessler, Special Agent, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 8:22 am a.m./p.m. *(specify reliable electronic means)*.

Date: May 10, 2023

Youlee Yim You
Judge's signature

City and state: Portland, Oregon

Honorable Youlee Yim You, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Description of the Premises, Property, Subject Vehicle, and Person to be Searched

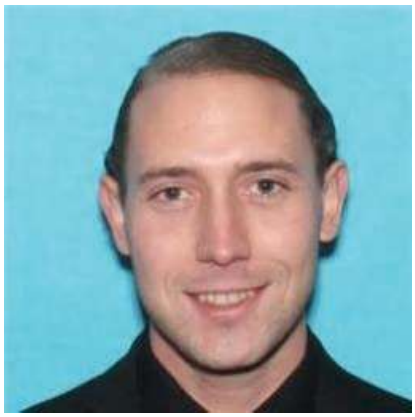
1. **Subject Premises:** 11304 SE 60th Ave., Milwaukie, OR 97222

The **Subject Premises** is a single-story three-bedroom, one bathroom house located at 11304 SE 60th Ave., Milwaukie, OR 97222. The house is light brown with dark brown trim and has an attached garage with a white door. The number 11304 can be seen in white letters hanging below the mailbox.

2. Subject Vehicle: Yellow Hummer 3 bearing Oregon license plate #392NAH.

3. Person

The person of Kyle Scott **BROADHURST** (and any cell phone or digital device on his person or under his control at the time of search, provided he is located in the District of Oregon at the time of the search), date of birth XX/XX/1985; a white male; approximately 5'10" and 160 lbs. See below photograph, which was obtained from **BRAODHURST's** Driver's License:



ATTACHMENT B

Items to be Searched For, Seized, and Examined

The following items, documents, and records that contain contraband or are evidence, fruits, or instrumentalities of violations of Title *18 U.S.C. § 2252A(a)(2)* – Distribution of Child Pornography and Title *18 U.S.C. § 2252A(a)(5)(B)* – Possession of or Accessing with Intent to View Child Pornography (the "**Target Offenses**"), including:

I. Digital Evidence

1. Any mobile devices including cell phones belonging to or used by Kyle Scott **BROADHURST**, that may have been used to commit or facilitate the **Target Offenses**;

2. Any computers belonging to or used by **BROADHURST** that may have been used to facilitate violations of the **Target Offenses**, including any peripheral devices such as external hard drives, external disk drives, power supplies, modem, and routers;

3. Any computer equipment or digital devices belonging to or used by **BROADHURST,** that are capable of being used to create, access, or store contraband or evidence, or are fruits or instrumentalities of the **Target Offenses**, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

4. Any magnetic, electronic, or optical storage device belonging to or used by **BROADHURST** that is capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and

cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband, or evidence, or are fruits or instrumentalities of such crimes;

5. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

6. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

7. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

8. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, digital devices, storage devices, cloud-based storage accounts, or data; and

9. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; screen names or usernames, and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

II. Records, Documents, and Visual Depictions

10. Any records, documents, or materials, including correspondence, that pertain to any account, record, data, or file related to any peer-to-peer (P2P) file sharing network accessed by **BROADHURST.**

11. Any records, documents, or materials, including account login information and/or passcodes related to any P2P file sharing network account belonging to, controlled by, or accessed by **BROADHURST.**

12. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

13. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

14. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

15. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

16. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

17. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

18. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;

19. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images or videos sent or received; and

20. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or notes associated with child pornography or those who collect, disseminate, or trade in child pornography.

As used above, the terms records, documents, programs, applications, or materials includes records, documents, programs, applications, or materials created, modified or stored in any form including digital or electronic form.

Search Procedure

23. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *Unlocking of the cell phone using biometrics, if applicable*. Law enforcement officers will attempt to unlock digital devices including cell phones that have biometric capabilities.

Investigators will accomplish this by either holding the fingers to digital device(s) equipped with a fingerprint authentication feature, or holding the digital device(s) equipped with a facial recognition authentication feature to **BROADHURST's** face. This will enable investigators to access the phone which may be difficult otherwise and search the contents as authorized by the warrant.

b. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and herein.

c. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

d. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

e. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and herein. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

f. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to

exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

g. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of time from the Court within the original 120-day period from the date the warrant was executed. The government shall complete the search of the digital device or image within 180 days of the date the warrant was executed. If the government needs additional time to complete the search, it may seek an extension of time from the Court.

h. If, at the conclusion of the search, law enforcement personnel determine that specific files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining

to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

i. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

DISTRICT OF OREGON)
) ss: AFFIDAVIT OF RACHEL KESSLER
County of Multnomah)

Affidavit in Support of an Application for a Search Warrant

I, Rachel Kessler, being duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I have been employed as a Special Agent (SA) by the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) since March 2021. I am currently assigned to the child exploitation unit in the HSI office in Portland, Oregon. My formal law enforcement training includes successfully completing a six-month training program including the completion of the Criminal Investigator Training Program (CITP) and the HSI basic training course at the Federal Law Enforcement Training Center in Brunswick, Georgia. During the training, I learned about child exploitation investigations and ways to conduct them. During my post-academy training, I have become familiar with ways that child pornography is shared, distributed, and/or produced, including the use of various social media websites (Facebook, Twitter, Kik, Snap Chat, Discord, MEGA, etc.), "cloud" based storage, and peer-to-peer (P2P) networks. Often, individuals involved in child exploitation will collect or store images and/or videos on various media devices they keep at their residences, or in offsite locations such as "cloud" based storage. I have also become familiar with some of the jargon or slang terms that people involved in child exploitation will use to discuss their activities.

2. I have also worked with agents conducting investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of a suspect's premises and assisted in gathering evidence pursuant to

search warrants, including search warrants in child pornography investigations. I have participated in interviews of persons who attempt to possess and/or distribute child pornography.

3. Prior to becoming an HSI Special Agent, I was employed by United States Customs and Border Protection (CBP) as a Customs and Border Protection Officer (CBPO). As a CBPO I enforced the customs and immigration laws of the United States. I performed primary and secondary examinations of passengers and conveyances entering the United States. I utilized a variety of basic and advanced tools and interviewing techniques to determine whether to admit a person to the United States or refer them for further examination. Additionally, I used my interviewing techniques to gather pertinent information to deny people entry to the United States for violating or attempting to violate various U.S. customs and immigration laws.

4. I submit this affidavit in support of an application for a warrant authorizing searches of Kyle Scott **BROADHURST's** person, any devices found on his person, including his cell phone, the **Subject Vehicle** (a yellow Hummer 3 bearing Oregon license plate #392 NAH), and the **Subject Premises** located at 11304 SE 60th Ave., Milwaukie, OR 97222, as described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) – Distribution of Child Pornography and 18 U.S.C. § 2252A(a)(5)(B) – Possession of or Accessing with Intent to View Child Pornography, collectively referred to as the "**Target Offenses**," as described in Attachment B.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who have

knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

6. *Title 18, United States Code, § 2252A(a)(2)*: makes it a crime to knowingly receive or distribute child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. *Title 18, United States Code, § 2252A(a)(5)(B)* makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. "Child pornography," as defined in 18 U.S.C. § 2256(8), includes any visual depiction of a child under the age of 18 years engaging in sexually explicit conduct. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal, whether between members of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals, anus, or pubic area of any person.

Background on Computers and Child Pornography

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have drastically changed how child pornography is produced and distributed.

10. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

11. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer using a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

12. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously in the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person or inside their vehicle.

13. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs such as Kik, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs such as LimeWire and eMule, and networks such as eDonkey, Gnutella, ARES, Tumblr, and BitTorrent, among others. Collectors and distributors of child pornography sometimes also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set

up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet and can access stored files using any device capable of connecting to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

14. An Internet Protocol (IP) address is a unique number that devices such as computers, routers, Internet fax machines, printers, and the like use to identify and communicate with each other over a network. An IP address can be thought of as a street address. Just as a street address identifies a particular building, an IP address identifies a particular Internet or network access device. When a user logs on to his/her Internet Service Provider (ISP), they are assigned an IP address for the purpose of communication over the network. An IP address can be statically assigned, meaning the IP address does not change from one Internet session to another, or dynamically assigned, meaning a user receives a different IP address each time the user accesses the Internet. An IP address can only be assigned to one user at a time, and ISPs keep records of who IP addresses are assigned to by date and time. Similarly, cell phone service providers also generally keep IP records that can identify what device (cell phone) utilized the IP address on a certain date and time.

15. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer

user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

16. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

17. I also know from my training and experience that many people who download child pornography from the Internet, and those who collect child pornography, frequently save images and videos of child pornography on their computers and/or transfer copies to other computers and storage media, including cloud storage accounts, external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child pornography investigations to find child pornography on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

18. I know based on my training and experience that many social media applications, such as Facebook, Instagram, Twitter, Snap Chat, Kik messenger and others can be directly accessed and used with one's cellular phone. Often, these applications require the user to download the application directly to their phone, which then allows seamless use between the cellular phone and the social media website.

Peer-to-Peer (P2P) File Sharing

19. Peer-to-peer file sharing (P2P) is a method of communication available to Internet users using special software. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the internet. There are multiple types of P2P file sharing networks on the internet including eMule, Gnutella, eDonkey, ARES, and BitTorrent. P2P file sharing networks are frequently used to trade digital media files of child pornography, including both videos and images.

20. To connect to a particular P2P file sharing network, a user first obtains the P2P client software program for a particular P2P file sharing network, which is publicly available and can be downloaded from the Internet. A particular P2P file sharing network may allow access to the network through many different P2P client software programs. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks.

21. When P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide network for download. However, a user may modify settings to disable the sharing function. A user searches for and obtains files by conducting keyword searches of the P2P file sharing network. When a user initially logs onto the P2P network, a list of the files that the user

is sharing is transmitted to the network. The P2P file sharing software then matches files in these lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search to locate certain types of files. For example, pedophiles searching for images of child pornography may type in "PTHC." I know from training and experience that this stands for "Preteen Hard Core," which is a way to designate child pornography. Collectors of child pornography are usually aware of the fact that using this search term will locate images or videos that contain child pornography. The results of the keyword search are displayed, and the user then selects the files that they want to download.

22. The download of a file can be achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a user downloads a file, it is stored in the area previously designated as a "shared" folder by the user and will remain there until moved or deleted by the user.

23. Most of the P2P file sharing software applications keep logs of each download event. Thus, a person interested in sharing child pornography with others in the P2P file sharing network need only place those files in their "shared" folder(s), and those child pornography files are then available to all users of the P2P file sharing network for download regardless of their physical location. A P2P file transfer is assisted by reference to an IP address. The IP address provides a unique location making it possible for data to be transferred between computers.

24. The computers that are linked together to form the P2P file sharing network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce.

25. Even though the P2P network links together computers from all over the world and users can download files, it is not possible for one user to send or upload a file to another

user of the network. The software is specifically designed only to allow files to be downloaded that have been selected. A user does not have the ability to send files from their computer to another user's computer without the other user's permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without the other user's active participation.

26. One of the advantages of P2P file sharing is that multiple files may be downloaded at one time. In addition, a user may download a file from numerous sources at once, thereby reducing the time it takes to download a file. For that process to work, the P2P network software assigns a "hash value," or digital fingerprint, to the file being downloaded.[1] The software then searches the network for identical copies of that file (as determined by matching hash values), sends parts of the file to the requesting computer from multiple sources, then reassembles the complete file on the requesting computer. A keyword search in the eMule, BitTorrent, Gnutella, or Gnutella 2 software could also result in a list of files that meet the search criteria sorted by hash value. Special law enforcement P2P software programs can then search the P2P network for hash values known to depict child pornography and can download those files. Unlike publicly available versions of the P2P software, the law enforcement version is designed to download files from a single source only.

[1] A hash value is a lengthy mathematical algorithm that represents a file's digital fingerprint or digital DNA. Two files whose contents are identical will have matching hash values, even if their file names are different. However, any modification of a file's content, however minor, will result in a completely different hash value, even if the file name is unchanged. Thus, if two files have matching hash values, they are considered bit-for-bit identical.

Statement of Probable Cause

HSI Portland Receives Investigative Lead from Retired Police Detective

27. In April 2023, I received information from the Milwaukie, Oregon, Police Department (MPD) regarding an IP address that was identified as sharing suspected child pornography over various P2P file sharing networks including eMule, BitTorrent, Gnutella, and Gnutella2. This investigation focuses mainly on the suspected child pornography downloads from the P2P file sharing network eMule.

28. Several weeks ago, MPD received information from the Multnomah County Sheriff's Office (MCSO) that a user at the IP address 73.67.139.115 (the "**Target IP Address**") was offering to share child pornography on P2P file sharing networks. MCSO had received that information from a civilian that had identified the **Target IP Address** on multiple P2P networks as offering to share suspected child pornography.[2] Upon receiving the information from the civilian, MCSO submitted a subpoena to Comcast for subscriber information for the **Target IP Address** and two other IP addresses (173.164.109.86 and 173.8.221.190) linked to the downloads.[3]

[2] The civilian is a retired law enforcement officer who now works in the private sector training law enforcement officers in investigating the sharing of child pornography via P2P networks. I believe the information provided by the civilian to be reliable and credible to the extent that it has been corroborated by this investigation.

[3] The IP address 173.164.109.86 was subscribed to Time Inc., which is a business located at 8039 SE 17th Ave, Portland, OR. The IP address 173.8.221.190 was subscribed to Sellwood Saloon located at 8301 SE 17th Ave, Portland, OR. From my experience and in talking with other law enforcement officers familiar with P2P investigations, I believe the user was most likely downloading suspected child pornography while they were at the bar or business.

29. In response to the subpoena, Comcast reported that the **Target IP Address** was subscribed to Carol Leah Broadhurst at 11304 SE 60th Ave., Milwaukie, OR 97222 (**Subject Premises**) which is further discussed below. Since the **Subject Premises** appeared to be outside of MCSO's jurisdiction, they transferred the case to MPD for further investigation.

30. During law enforcement database checks, MPD learned that **Kyle Scott BROADHURST** (born XX-XX-1985) also appeared to reside at the **Subject Premises**. MPD later learned that **BROADHURST** is Carol Broadhurst's son. According to criminal history inquiries, **BROADHURS**T is a registered sex offender who had previously been investigated by HSI Portland. MPD then contacted HSI Portland for investigative assistance.

31. After I received the above information from MPD, I learned that the Linn County, Oregon, Sheriff's Office (LCSO) had downloaded files containing child pornography from the **Target IP Address** multiple times between March 26, 2023, and April 2, 2023. LCSO conducts proactive investigations on various P2P networks by using undercover computers to locate and download files known to contain child pornography. HSI SA Clinton Lindsly requested the LCSO downloads for review.

Review of Downloaded Files from the Target IP Address

32. On April 19, 2023, I received and reviewed five files LCSO downloaded from the **Target IP Address.** Additionally, LCSO included a "Detailed Log" for each downloaded file that included information such as unique identifiers for the file that was downloaded, the IP address that the suspect device was utilizing, the name of the file that was being downloaded, as well as date and time the file was downloaded. During the review I identified three videos that met the federal definition of child pornography. I was unable to view one of the other two files;

the final file did not contain child pornography. Descriptions of the three child pornography files follows:

a. **Downloaded from the Target IP Address on March 26, 2023**

   i. File Hash: C7656316DAA13572E6C45DA62BF49DC6

   ii. File Name: babyshivid5-owl.avi

   iii. Duration: One minute

   iv. Description: A video that depicted an adult male vaginally penetrating a prepubescent girl with his erect penis. In the video the girl can be heard crying.

b. **Downloaded from the Target IP Address on March 26, 2023**

   i. File Hash:81E84A2FC68E91CF259317F11A2B9C54

   ii. File Name: 2014-5_toddlerpussyplay01.AVI

   iii. Duration: Five minutes, 39 seconds

   iv. Description: A video that depicted an adult hand inserting what appeared to be a small red pepper into a pre-pubescent girl's vagina. The adult hand can also be seen touching and inserting its fingers into the girl's vagina.

c. **Downloaded from the Target IP Address on April 2, 2023**

   i. File Hash: CC0D7D9AFE2E6CD8019E2B2D62A6347C

   ii. File Name: [—m˜D] 7yo and 9yo girls play.avi

   iii. Duration: One minute, 20 seconds

   iv. Description: A video that depicted a pre-pubescent child performing oral sex on an adult male's erect penis.

IP Address Used to Share Child Pornography Subscribed to Subject Premises

33. On February 22, 2023, MCSO served a subpoena to Comcast for the subscriber records related to the **Target IP Address**. On March 8, 2023, Comcast responded that the **Target IP Address** was subscribed to Carol Leah Broadhurst at 11304 SE 60th Ave., Milwaukie, OR 97222 (**Subject Premises**). I then submitted another subpoena to Comcast for subscriber records related to the **Target IP Address** for each date / time that LCSO conducted an undercover download of child pornography as identified above. In each instance, the **Target IP Address** was subscribed to Carol Broadhurst at the **Subject Premises**. Carol Broadhurst has no criminal history.

BROADHURST identified as a Registered Sex Offender and Resident of the Subject Premises

34. **BROADHURST** is a registered sex offender following a conviction in October 2013 in the United States District Court for the District of Oregon for Possession of Child Pornography. **BROADHURST** was sentenced to 48 months in prison and 60 months of supervised release. **BROADHURST** was released from custody in or around 2017. His federal supervised release ended in approximately October 2020.

35. According to the Oregon State Police (OSP) sex offender registry, **BROADHURST** last registered as a sex offender on January 11, 2023. He listed his residence address as the **Subject Premises**, listed the cell phone number 503-739-3771 (**Subject Cell Phone**) and reported that he drives a yellow Hummer 3 bearing Oregon license plate #392 NAH (**Subject Vehicle**). **BROADHURST** also reported that on March 15, 2023, he was supposed to start working as a QC technician for Nuance Systems located at 17233 SW Kable Lane, Portland, OR 97224. As further discussed below, it appears that Nuance Systems relocated to a new facility located at 21020 SW Cipole PL., Sherwood, OR 97140.

HSI Serves Additional Subpoenas

36. I submitted an administrative subpoena to AT&T for subscriber information for the **Subject Cell Phone**. AT&T returned the following information:

a. Name: Kyle Broadhurst

b. Service Start Date: October 24, 2020

c. Contact Home Email: kavalierkyle@gmail.com

37. The records also listed two different addresses: 10439 SE Cook CT. Apt. 378, Portland, OR 97222 (Clackamas Trails Apartments) and the **Subject Premises**. I contacted the property manager for Clackamas Trails Apartments, who did not have any record of **BROADHURST** living there.

38. Additionally, I submitted an administrative subpoena to Google for subscriber information for the email address kavalierkyle@gmail.com. Google returned the following information:

d. Name: Kavalier Kyle

e. Created on: May 23, 2020

f. Recovery SMS: 503-739-3771 (**Subject Cell Phone**)

39. Google also provided IP connectivity logs for kavalierkyle@gmail.com. In reviewing the IP connectivity logs, I observed that from July 27, 2022, to April 25, 2023, the user of the email address kavalierkyle@gmail.com logged into their account using the **Target IP Address** approximately 135 times, which is consistent with residing at the **Subject Premises**. I also observed that on the April 2, 2023, the email address kavalierkyle@gmail.com logged into their account using the **Target IP Address**. This is the same day that LCSO downloaded suspected child pornography from the **Target IP Address**. As such, I believe that

BROADHURST is using a digital device, likely a computer, at the **Subject Premises**, and using the **Target IP Address** to distribute child pornography.

40. In addition, according to the Google IP connectivity logs, on April 25, 2023, the IP address used to login to the account was 192.65.141.133. That IP address is serviced by City of Sherwood Broadband. Investigators submitted an administrative subpoena to City of Sherwood Broadband for that IP address and learned that it was subscribed to NSI Mfg. at 21020 SW Cipole PL., Sherwood, OR 97140. According to an open-source query, NSI Mfg. is Nuance Systems LLC. Based on the IP connectivity logs for NSI Mfg. in Sherwood, OR it appeared **BROADHURST** changed work locations.

41. On April 26, 2023, at approximately 10:43 a.m., SA Lindsly conducted surveillance at NSI Mfg. at 21020 SW Cipole PL., Sherwood, OR 97140. SA Lindsly observed a yellow Hummer bearing Oregon License plate# 392 NAH (**Subject Vehicle**) parked at the business. According to the Oregon Department of Motor Vehicles, the vehicle is registered to **BROADHURST** at the **Subject Premises**.

Surveillance of the BROADHURST and Further Identification of the Subject Premises

42. On April 27, 2023, MPD Detectives conducted surveillance of **BROADHURST**. During the day, MPD Detectives located the **Subject Vehicle** at NSI Mfg in Sherwood, OR. At approximately 3:38 p.m., **BROADHURST** was seen departing his place of employment, getting in the **Subject Vehicle,** and driving away. At approximately 5:15 p.m., MPD Detectives observed **BROADHURST** park and go into "Jakes Place," a bar located at 8039 SE 17th Ave., Portland, OR 97202. Jakes Place is located approximately .2 miles from Sellwood Saloon. As stated previously, a civilian had identified an IP address subscribed to the Sellwood Saloon that that was accessing the P2P network and offering to share child pornography.

43. On May 01, 2023, MPD conducted additional surveillance of the **Subject Premises**. At approximately 6:26 a.m., investigators saw **BROADHURST** leave the residence, get into the **Subject Vehicle,** and drive away.

44. Based on my training and experience and **BROADHURST**'s previous federal conviction, I believe **BROADHURST** is likely the user of the device that is accessing the P2P file sharing network to share child pornography at the **Target IP Address** and resides at the **Subject Premises**. I also believe that evidence of the **Target Offenses** will likely be found on **BROADHURST**'s person, in the **Subject Vehicle**, or at the **Subject Premises**. It appears that **BROADHURST** drives the **Subject Vehicle** often and previous downloads from his computer via a P2P network occurred while **BROADHURST** was logged into his account from locations other than the **Subject Premises**, including businesses in an area in which **BROADHURST** was seen frequenting. Additionally, according to a Report of Investigation written by HSI Portland, during the execution of their search warrant in 2011, BROADHURST admitted that he accessed other people's open wireless access points to try and remain undetected by law enforcement.

45. Thus, I believe **BROADHURST** transports and/or uses the device(s) while in the **Subject Vehicle**. Moreover, I know, based on my training and experience, that many digital data storage devices are quite small and are easily concealed and transported in a vehicle. I therefore request that a search of the **Subject Vehicle** be included in the scope of this warrant.

Search and Seizure of Digital Data

46. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

47. Based on my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

48. I know from my training and experience, as well as from information found in publicly available materials, that these digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint, or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as biometric authentication and their availability is dependent on the model of the device as well as the operating system on the device. If a user enables biometric authentication on a digital device, he or she can register fingerprints, or their face, to unlock that device.

49. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) when too many hours have passed since the last time the device was unlocked; and (5) when the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time. Thus, in the event law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

50. The passcode or password that would unlock any devices on **BROADHURST**'s person, in the **Subject Vehicle** or at the **Subject Premises**, is not known to law enforcement. Thus, it is necessary to press the fingers of **BROADHURST**'s to the any phones device's sensor, or hold the phone up to **BROADHURST**'s face, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. I therefore request that the Court authorize law enforcement officers to press **BROADHURST'S** fingers or thumbs to the sensor of any phones or digital devices equipped with fingerprint authentication, or to hold any device equipped with facial recognition authentication up to **BROADHURST**'s face, in order to conduct the search authorized by this warrant.

Removal of Data Storage Devices

51. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for various reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all the necessary technical

manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive; the larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can make doing an on-site search impractical.

Laboratory Setting May Be Essential for Complete and Accurate Analysis of Data

52. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

53. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and

analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant period, can help determine who was sitting at the keyboard.

54. *Latent Data:* Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten

by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

55. *Contextual Data*:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal

information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

56. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On site search, if practicable*. Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if computer personnel that are on-site determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that

they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of time from the Court within the original 120-day period from the date the warrant was executed. The government shall complete the search of the digital device or image within 180 days of the date the warrant was executed. If the government needs additional time to complete the search, it may seek an extension of time from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data

that fall within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

Items to be Seized

57. To search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or

to create, access, process, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as thumb drives and other USB data storage devices, floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the computer equipment, storage devices, or data, and any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

g. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite

web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

Retention of Image

58. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

59. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

60. The government has made no prior effort in any judicial forum to obtain the materials sought in this requested warrant.

Conclusion

61. Based on the foregoing, I have probable cause to believe that Kyle **BROADHURST** committed violations of *18, U.S.C. § 2252A(a)(2)* – Distribution of Child Pornography, and *18 U.S.C. § 2252A(a)(5)(B)* – Possession of or Accessing with Intent to View Child Pornography, and that contraband and evidence, fruits, and instrumentalities of those

violations, as described in Attachment B, will be located on **BROADHURST's** person, any devices found on **BROADHURST**'s person, including any cell phones or digital devices, the **Subject Vehicle**, and the **Subject Premises**, as described in Attachment A. I therefore respectfully request that the Court issue a warrant authorizing a search of **BROADHURST**'s person, the **Subject Vehicle**, and the **Subject Premises**, as described in Attachment A, for the items listed in Attachment B, and authorizing the examination and seizure of any such items found.

62. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney Gary Sussman. AUSA Sussman advised me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

(By telephone)
Rachel Kessler, Special Agent
Homeland Security Investigations

Sworn to before me telephonically or by other reliable means pursuant to Fed. R. Crim. P. 4.1 at 8:22 a.m. am/pm on May 10, 2023.

Youlee Yim You
HONORABLE YOULEE YIM YOU
United States Magistrate Judge